



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

| | | |
|--|-----------|---|
| (51) International Patent Classification ⁶ : H04L 9/30 | A1 | (11) International Publication Number: WO 98/49804 (43) International Publication Date: 5 November 1998 (05.11.98) |
| (21) International Application Number: PCT/US98/08299 (22) International Filing Date: 24 April 1998 (24.04.98) (30) Priority Data: 08/842,080 28 April 1997 (28.04.97) US (63) Related by Continuation (CON) or Continuation-in-Part (CIP) to Earlier Application US 08/842,080 (CIP) Filed on 28 April 1997 (28.04.97) (71) Applicant (for all designated States except US): CERTCO LLC [US/US]; 22nd floor, 55 Broad Street, New York, NY 10004 (US). (72) Inventors; and (75) Inventors/Applicants (for US only): FRANKEL, Yair [US/US]; 64 Pomander Walk, Ridgewood, NJ 07450 (US). YUNG, Marcel, M. [IL/US]; 605 West 112th Street, New York, NY 10025 (US). (74) Agents: HUANG, Stuart, T., F. et al.; Steptoe & Johnson, LLP, 1330 Connecticut Avenue, N.W., Washington, DC 20036 (US). | | (81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG). Published With international search report. |
| (54) Title: OPTIMAL-RESILIENCE, PROACTIVE, PUBLIC-KEY CRYPTOGRAPHIC SYSTEM AND METHOD (57) Abstract <p>Proactive robust threshold schemes are presented for general "homomorphic-type" public key systems, as well as optimized systems for the RSA function. Proactive security employs dynamic memory refreshing and enables us to tolerate a "mobile adversary" that dynamically corrupts the components of the systems (perhaps all of them) as long as the number of corruptions (faults) is bounded within a time period. The systems are optimal-resilience. Namely they withstand any corruption of minority of servers at any time-period by an active (malicious) adversary (i.e., any subset less than half. Also disclosed are general optimal-resilience public key systems which are "robust threshold" schemes (against stationary adversary), and are extended to "proactive" systems (against the mobile one). The added advantage of proactivization in practical situations is the fact that, in a long-lived threshold system, an adversary has a long time (e.g., years) to break into any t out of the l servers. In contrast, the adversary in a proactive systems has only a short period of time (e.g., a week) to break into any t servers. The model of mobile adversary seems to be crucial to such "long-lived" systems that are expected to span the secure network and electronic commerce infrastructure.</p> | | |

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | | | |
|----|--------------------------|----|--|----|--|----|--------------------------|
| AL | Albania | ES | Spain | LS | Lesotho | SI | Slovenia |
| AM | Armenia | FI | Finland | LT | Lithuania | SK | Slovakia |
| AT | Austria | FR | France | LU | Luxembourg | SN | Senegal |
| AU | Australia | GA | Gabon | LV | Latvia | SZ | Swaziland |
| AZ | Azerbaijan | GB | United Kingdom | MC | Monaco | TD | Chad |
| BA | Bosnia and Herzegovina | GE | Georgia | MD | Republic of Moldova | TG | Togo |
| BB | Barbados | GH | Ghana | MG | Madagascar | TJ | Tajikistan |
| BE | Belgium | GN | Guinea | MK | The former Yugoslav Republic of Macedonia | TM | Turkmenistan |
| BF | Burkina Faso | GR | Greece | ML | Mali | TR | Turkey |
| BG | Bulgaria | HU | Hungary | MN | Mongolia | TT | Trinidad and Tobago |
| BJ | Benin | IE | Ireland | MR | Mauritania | UA | Ukraine |
| BR | Brazil | IL | Israel | MW | Malawi | UG | Uganda |
| BY | Belarus | IS | Iceland | MX | Mexico | US | United States of America |
| CA | Canada | IT | Italy | NE | Niger | UZ | Uzbekistan |
| CF | Central African Republic | JP | Japan | NL | Netherlands | VN | Viet Nam |
| CG | Congo | KE | Kenya | NO | Norway | YU | Yugoslavia |
| CH | Switzerland | KG | Kyrgyzstan | NZ | New Zealand | ZW | Zimbabwe |
| CI | Côte d'Ivoire | KP | Democratic People's Republic of Korea | PL | Poland | | |
| CM | Cameroon | KR | Republic of Korea | PT | Portugal | | |
| CN | China | KZ | Kazakhstan | RO | Romania | | |
| CU | Cuba | LC | Saint Lucia | RU | Russian Federation | | |
| CZ | Czech Republic | LI | Liechtenstein | SD | Sudan | | |
| DE | Germany | LK | Sri Lanka | SE | Sweden | | |
| DK | Denmark | LR | Liberia | SG | Singapore | | |
| EE | Estonia | | | | | | |

OPTIMAL-RESILIENCE, PROACTIVE, PUBLIC-KEY CRYPTOGRAPHIC SYSTEM AND METHOD

FIELD OF THE INVENTION

The invention relates to the field of electronic cryptographic systems and methods. More particularly, the invention relates to systems and methods for distributing a cryptographic service (e.g., electronic document signing) among a plurality of servers in a communication or data processing network.

BACKGROUND OF THE INVENTION

Certain attempts at distributed cryptographic operation, such as signing and encrypting/decrypting, are known. However, no previous system enjoys efficiency of operation combined with high level of security and availability in a system that retains its security while any minority of distributed servers collude and stop, misbehave, and try to help in breaking the system's secret. Other attempts have been made to deal with various issues of threshold cryptography and mobile adversaries, although only a limited number discuss proactive function sharing.

The notion of "proactive public-key" was addressed in A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung in: *Proactive Secret Sharing, or: How to Cope with Perpetual Leakage*, Advances in Cryptology - Crypto 95 Proceedings, Lecture Notes in Computer Science, Vol. 963, D. Coppersmith ed., Springer-Verlag, 1995, pp. 339-352 ("[HJKY]"). This implementation was based on "discrete logarithm" with exponentiation in a prime field (i.e., given the elements modulo a prime p , use a generator of $GF(q)$ where q divides $p - 1$). This problem involves distributed computation over keys, and the keys in this case are taken from domains whose algebraic structure is public (a group of a known order).

A number of other theoretic references to making cryptographic mechanisms proactive include: R. Ostrovsky and M. Yung, *How to Withstand Mobile Virus Attacks*, Proc. of the 10th ACM Symposium on the Principles in Distributed Computing,

(2)

1991, pp. 51-61 ("[OY]"); R. Cannetti and A. Herzberg, *On Maintaining Security in the Presence of Transient Faults*, Advances in Cryptology, Proc. of Crypto '94 ("[CH]"); A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung, *Proactive Public Key and Signature Systems*, The 4-th ACM Symp. on Comp. and Comm. Security, April 1997 ("[HJKY]"); Y. Frankel, P. Gemmel, P. MacKenzie and M. Yung, *Proactive RSA*, Tech Report Version SAND96-0856, Sandia National Laboratories, March 1996 ("[FGMY]"). Each of the references cited above, and all other references cited below, are fully incorporated herein by reference.

SUMMARY OF THE INVENTION

The invention offers a general implementation of distributed cryptographic functions combined with a high level of availability of service, high efficiency of operation, and a high level of security. It is applicable to a variety of asymmetric-key cryptographic functions, such as digital signatures, encryption, escrow, authorization, etc.

An object of the invention is to provide a cryptographic system and service that is distributed and optimal in tolerance of faulty distributed components.

A further object is to provide an asymmetric-key cryptographic system and service employing a plurality of servers such that the system is available and remains secure as long as, within a time-period, some majority of the servers acts correctly.

A further object is to provide an asymmetric-key cryptographic system and service having a set of protocols for distributing a cryptographic function.

A further object is to provide an asymmetric-key cryptographic system and service capable renewing and recovering key shares.

A further object is to provide an asymmetric-key cryptographic system and service having optimal resilience.

A further object is to provide a robust cryptosystem.

(3)

These and other objects are achieved by providing a distributed cryptographic system and service including periodic reexpression of the basic cryptographic function. The reexpression may be to a different family of functions than the basic cryptographic function. Reexpression may utilize a "share of shares" method (e.g., "poly-to-sum" or "sum-to-poly"). These methods allow for proactivization, and for changing the threshold parameter from t -out-of- l to t -out-of- t and vice versa. The methods further provide for changing t and l dynamically as a system management tool. Additional aspects of the invention provide for checking protocols to monitor individual servers of the distributed cryptographic system, thereby making the system robust.

Techniques of the present invention can be applied to any system implementing a cryptographic function where: 1) the function has the property of share translation (i.e., $f_{k1}(m) * f_{k2}(m) = f_{k1 \cdot k2}(m)$); 2) one can compute inverses in the share space; and 3) the share space is simulatable (i.e., one can choose random elements in a simulatable space which is indistinguishable from choosing in the key space).

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates a network environment that has available to it a distributed cryptographic service function or functions and that is suitable for embodying the present invention.

Fig. 2 illustrates an exemplary request by a requesting node to the distributed system for a cryptographic service.

Fig. 3 illustrates an exemplary distributed system for performing a cryptographic service.

Fig. 4 illustrates generic communications within a distributed system for embodying present invention.

Fig. 5 illustrates general phases of operation of a distributed system embodying the present invention.

Fig. 6 illustrates a system of communicating servers.

(4)

Fig. 7 illustrates the re-expression of an RSA function.

Fig. 8 illustrates a checking protocol for a robust cryptographic system.

Fig. 9 illustrates an arrangement that provides an additional layer of protection in consideration of non-trusting entities.

Fig. 10 illustrates reshuffling in a distributed system.

Fig. 11 illustrates a distributed system having changes in the number of users and threshold.

Fig. 12 illustrates the notion of sharing of a general homomorphic function.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Threshold cryptography in general, and function sharing for public-key functions in particular, has the spirit of secret sharing, where a secret is shared and is recoverable only from a threshold of shareholders. Function sharing provides for the availability of a keyed cryptographic function $f_k(\cdot)$ by distributing $f_k(\cdot)$ to a set of l servers such that, for any valid argument m , any set of at least a threshold of t out of the l servers can compute $f_k(m)$. This increases the availability of function evaluation (typically a signature or a decryption function). For security, an adversary who (1) controls less than a threshold of servers and (2) can hear all public messages obtains no computational advantage in computing $f_k(m')$ for a target message m' (as compared to an adversary attacking the centralized function $f_k(\cdot)$ with the same capabilities). Thus the function is protected by "space diffusion," because an attacker is forced to break the memory of more than a threshold t of the function shareholders.

"Resilience" is a property describing the number of allowed compromised and misbehaving servers in a time period, which is a parameter here called t . An optimal t ("optimal resilience") means that the total number of servers is $l \geq 2(t - 1) + 1$. For this t , a majority of arbitrarily misbehaving

(5)

servers can "control" the computation (even for a stationary adversary).

The notion of "proactive security" (against a mobile adversary) provides enhanced protection of memories of long-lived cryptographic keys that may be distributed (i.e., protected by "space diffusion"). Proactive security adds protection by "time diffusion" as well. Namely, given a distributed function via threshold cryptography (function sharing) as described above, it adds a periodic refreshing of the contents of the distributed servers' memories. This refreshing is a " t -wise re-randomization" of the local servers' values in a way that preserves the global key, but makes previous contents of any set of less than t out of the l servers "useless". This renders useless the knowledge of the mobile adversary (e.g., hackers, viruses, bad administrators, etc.) obtained in the past from compromising less than the allowed t servers, and gives the system a self-securing nature.

The proactive systems for cryptographic functions inherit the availability of function-sharing by allowing any subset of servers of size t to compute the underlying function, thereby preventing a small set of faulty servers from disrupting availability. Proactive systems also can use robustness techniques to enhance availability of threshold cryptosystems by tolerating (detecting or correcting) malicious servers who are actively attacking the availability of the system. Moreover, proactive security enhances robustness, because it also provides for recovery of servers' memories that were previously corrupted by an adversary or by non-malicious faults. This gives the system a self-healing nature.

As a result, the system can tolerate a "mobile adversary" which is allowed to potentially move among servers over time, with the limitation that it can only control up to $t - 1$ servers during a particular time interval. The adversary may even eventually visit the entire system (under the above restriction). Nevertheless, the system self-heals from erasures and corruption of memories by the adversary, and

(6)

self-secures against the adversary's actions. This is a stronger adversary than a stationary one (which corrupts servers in a monotone fashion).

Fig. 1 illustrates a network environment that has available to it a cryptographic service function or functions and that is suitable for embodying the present invention. The network 101 includes multiple nodes 103 interconnected by communications paths 105. A distributed system 107 also connects to the network 101 through communication paths 109. It will be appreciated that many configurations of nodes 103 and connection paths 109 would be suitable.

Fig. 2 illustrates an exemplary request by a requesting node 111 to the distributed system 107 for a cryptographic service. As illustrated, a single requesting node 111 provides an input communication 113 to the distributed system 107. The distributed system 107 performs the cryptographic service, and returns an output communication 115. It will be appreciated that many variations in the manner of presentation of a request and return of a result would be suitable. For example, it is not required that a single requesting node 111 present a complete request in a single input communication 113, or that the output be returned to the requesting node 111 in a single output communication 115. Many protocols would be suitable, and could include a variety of administrative interactions, such as verification by the distributed system 107 of the identity of the requesting node 111, confirmation of payment for the service, etc.

Fig. 3 illustrates an exemplary distributed system 107 for performing a cryptographic service. Multiple agents 121 each participate in performing the cryptographic service in a distributed manner. For simplicity of illustration, all agents are given the same reference numeral, even though each might perform different functions in the course of providing a cryptographic service as discussed more fully below. An input

(7)

processor 123 receives an input communications 113 from a requesting network entity (not shown), and provides all of the agents 121 with information relating to the particular cryptographic service request. An output processor 125 receives and combines partial-result information from each of the agents 121, and provides an output communication 115 to the requesting network entity (not shown). The input processor 123 and output processor 125 can provide a layer of security as a so-called "firewall" between the network (not shown) and the agents 121, and can further assume additional administrative tasks.

Many cryptographic services involve the application of an asymmetric cryptographic key to input information. For example, if the cryptographic service is digital signing of electronic documents, the distributed system would generate a single signature for the document on behalf of the distributed system as a whole. In a public key cryptosystem, such a signature would correspond to the application of a secret signature key to a message. A signature recipient could verify the signature by using a public verification key that corresponds to the secret signature key.

In the distributed system 107, the secret signature key does not exist as a single key in a single location. Instead, a key distributor (sometimes called a "dealer") 127 distributes key shares to each of the agents 121. Each agent 121 applies its individual key share to an input, and the collective operation of multiple agents 121 would produce a single signature that can be verified by a single public verification key. However, no single agent possesses sufficient information to generate the signature by itself. Agents can also be referred to as "shareholders," in the sense that each agent holds a share of the key.

For the purpose of the illustration of Fig. 3, heavy lines with arrows at both ends designate a plurality of communication paths to all agents. Light lines without arrows

(8)

designate individual communication lines among agents. Each agent 121 can communicate with every other agent 121, with the key distributor 127, with the input processor 123, and with the output processor 125. It is preferred that no agent 121 be accessible to the network (not shown), except through the input processor 123 and output processor 125.

It will be appreciated that the methods of the present invention will be practicable in a variety of alternate configurations. For example, a single computer server could function both as an input processor 123 and an output processor 125. It is also possible (though not preferred) for a designated one or ones of the agents 121 to act as an input processor, or an output processor, or both. It is possible (though not preferred) for one of the agents to perform the key distribution function, rather than to rely on a separate key distributor 127. Alternatively, the agents might generate key shares in a distributed manner, in which case the key distributor 127 or one or more of the agents 121 could serve as an administrative coordinator for the key distribution process.

As will be discussed more fully below, the distributed system 107 can provide a cryptographic service using fewer than all agents 121. Fig. 4 illustrates generic communications within the distributed system 107 when three agents 131, 133 and 135 participate in providing the service. Two other agents 132, 134 do not actively participate in generating the output. In this illustration, the input processor 123 provides a message M to all five agents 131, 132, 133, 134, 135. Two of the five agents 132, 134 take no action, either because of an instruction from the input processor 123, or by some other signaling means. For example, the message itself could designate, or be associated with a header that designates, which particular ones of the agents are to participate in the service. Depending on the protocol used, as many as all of the processor can act, though only a

(9)
subset are used for the final computation. The three active agents 131, 133, 135 each apply their respective key shares to generate partial results 137. The output processor 125 receives the partial results 137 and combines them into an output $F_k(M)$, which in turn is communicated to the requesting node of the network (not shown).

Fig. 5 illustrates general phases of operation of the distributed system. In a setup phase 141, the key distributor distributes key shares to agents of the distributed system. In a function application phase 143, agents apply their respective key shares to inputs, and provide partial results to the output processor. In an update phase 145, members of the distributed system periodically take a variety of actions to maintain system security and to recover from passive failures and/or active attempts to corrupt the system. After the update phase 145, the distributed returns to providing cryptographic services in the function application phase 143.

Poly and Sums

A secret or a function may be shared via a system of mathematical equations, so as to enable subsets of users or a quorum of users to be able to apply their shares to get partial results that are then combined and computed upon to produce the final result. The final result on the given input is equal to the final result of the function which is re-expressed by the shares. The discussion below will concentrate on one representation of functions that are re-expressed as distributed shares, which are points on a polynomial (which we call sharing by "poly"). Other approaches are possible as in the use of finite geometry with hyperplanes.

A secret or a function may be shared so that all shares are needed and all shares are applied to get partial results that are then combined. We concentrate on combining

(10)

through addition, and therefore call this sharing: sharing by "sum."

A Secure Robust Threshold RSA

Described below is a threshold **RSA** scheme suitable for use in a distributed system as described above, but for which the security is not known. Then, the threshold scheme will be modified to be an **RSA** threshold scheme which is as secure as **RSA** under the stationary (non-mobile) adversary model. The basic idea of this example is to use the Shamir threshold scheme where inverse computations are easy.

RSA is generated by the dealer with a public key (e, n) and a private key d . Let $H = \gcd(e, L)$ and using the extended Euclidean algorithm compute P, s' such $1 = eP + \frac{L}{H} s'$. Note that $d \equiv P + Lk' \pmod{\theta(n)}$ where $k' \equiv ds' H^{-1} \pmod{\theta(n)}$. This is computable since H^{-1} exists because e must be invertible. A random polynomial $r(x)$ of degree $t - 1$ with coefficients in $\{0, L, \dots, L3tC\}$, where C is $\text{poly}(n)$, is chosen such that $r(I+1) = L \cdot k' \in \mathbb{Z}$. (The t factor in the coefficients is used for the proactive scheme and can be set to 1 for the static threshold RSA without proactivization.) Let P be made public (i.e., part of each share holder's key). Next, shadowholder i with public interpolation points $x_i = i$ receives secretly shadow $s_i = r(x_i) \in \mathbb{Z}$. Note, that the share is a multiple of L . Now, let Λ where $|\Lambda| = t$ be any subset of shareholders, observe:

$$d = P + \sum_{i \in \Lambda} s_i \cdot z_{i, \Lambda} \in \mathbb{Z} \quad \text{where} \quad z_{i, \Lambda} = \prod_{v \in \Lambda \setminus \{i\}} (x_i - x_v)^{-1} (I + 1 - x_v). \quad (1)$$

Since L divides s_i and $\prod_{v \in \Lambda \setminus \{i\}} (x_i - x_v)$ is a multiple of L , the terms in the above sum can be computed effectively over the integers from s_i (without inverses in the group). Hence to generate a signature for message m , each

(11)

$i \in \Lambda$ gives partial results $m^{s_i \cdot z_{i,\Lambda}} \bmod n$, and a combining function computes $m^p \bmod n$ and the final desired result: $m^d \equiv m^p \cdot \prod_{i \in \Lambda} m^{s_i \cdot z_{i,\Lambda}} \bmod n$. The above scheme is arithmetic-wise analogous to the systems in Y. Desmedt and Y. Frankel, *shared Generation of Authenticators and Signatures*, Advances in Cryptology -- Crypto 89 Proceedings, Lecture Notes in Computer Science, Vol. 435, G. Brassard ed., Springer Verlag, 1989, pp. 307-315 ("DF91") (which was designed for strong primes), the analogy is by distributing shares as s_i/L using interpolation point $I+1$ rather than 0 as the secret location and therefore choosing $z_{i,\Lambda}$ slightly different.

Shares of Shares (Poly to Sum)

Now is discussed a t -out of- t share (poly to sum) protocol. this is a protocol among t servers which transforms a t -out-of- 1 polynomial based sharing scheme to a t -out-of- t additive sharing scheme. It extends the scheme in [FGMY] which transforms a t -out-of- t sharing by sum to another t -out-of- t sharing by sum. This poly to sum protocol provides for randomization of the current state which converts the above (or [DF91]) to a secure system as discussed below in the section entitled "A Secure Threshold RSA Scheme." This randomization is also designed specifically to allow for robustness in the section below entitled "Robust Threshold RSA Scheme."

Fig. 6 illustrates a system of communicating servers 401, 403, 405, 407 and 409 which perform poly to sum for a 3 out of 5 sharing of the secret RSA key configuration. The secret RSA key is distributed using, for instance as in [DF91], a polynomial approach to sharing in which server 401 has share s_1 , server 403 has share s_2 , server 405 has share s_3 ,

(12)

server 407 has share s_4 , and server 409 has share s_5 . The poly-to-sum protocol enables any 3 of the servers to convert their respective shares for a 3 out of 1 system into a 3 out of 3 system. As denoted over time after the poly to sum protocol is performed, server 401 with share s_1 obtains share s_1' , server 405 with share s_3 obtains share s_3' , and server 407 with share s_4 obtains share s_4' . The new shares s_1' , s_3' , s_4' are obtained from a distributed protocol amongst the servers in the 3 out of 3 reconfiguration. The arrows in Fig. 6, denote that relationship of the new shares to the old shares. For example, server 401 obtains share s_1' by a protocol whose result has a relationship to s_1 , s_3 , and s_4 , as depicted in Fig. 6.

Fig. 7 illustrates the re-expression of an RSA function. The 3 out of 3 system configuration with servers 301, 303 and 305 depicts an additive three out of three sharing which can be performed after the poly to sum protocol is performed. That is, the keyed RSA function 309 is re-expressed into a protocol in which 301, 303, 305 working with server 307 can compute the same function evaluation of the keyed RSA as in 309. Let $d_1+d_2+d_3 \equiv d \pmod{\theta(n)}$, let server 301 have share d_1 , let server 303 have share d_2 and let server 305 have share d_3 . As depicted, each of the servers 301, 303 and 305 can compute $M^d \pmod n$ using their respective share, the input M , and the public composite n when working with 307. It is possible to allow server 307 to be server 301, 303 and/or 305.

To relate servers 401, 405 and 407 (Figure 6) to servers 301, 303 and 305 (Figure 7), after the poly to sum protocol, the configuration could be: server 401 depicted as server 301; 405 depicted as server 303; and server 407 depicted as 305. Moreover, share s_1' is replaced by d_1 , share s_2' is replaced by d_2 , and share s_3' is replaced by d_3 in Fig. 7. System implementation can be as follows.

(13)

Setup: We assume that the dealer, during share distribution, publishes elements $g, g_1 \in Z_n^*$ of maximal order, and it publishes $S_i = g^{s_i} \cdot L^2 \pmod n$ for all i . Let Λ where $|\Lambda| = t$ be the shareholders (servers) participating in the share of shares protocol. Servers choose a leader serve i' .

Sharing shares: Server i :

- Generates: $r_{i,j} \in_R \{0, 1, \dots, (n-1)\}$ for $j \in \Lambda \setminus \{i\}$.
- Set self-held share to be: $r_{i,i} = s_i \cdot Z_{i,\Lambda} - \sum_{j \in \Lambda \setminus \{i\}} r_{i,j} \in Z$.
- Privately transmit over the public channel using probabilistic encryption (an act which also publicly commits to the message) $r_{i,j} \in Z$ and $r'_{i,j} \in_R \{0, \dots, n-1\}$ to server j .

- Publish $R_{i,j} \equiv g^{r_{i,j} \cdot L^2} g_1^{r'_{i,j}}$, and $U_i \equiv \prod_{j \in \Lambda} g_1^{r'_{i,j}}$.

Verify and generate shares: Let $r_{i,j,0}$ and $r'_{i,j,0}$ be the commitment values that j received privately from i . This verifies that one received the correct committed values, shares are of correct size, and algebraic relations between various committed values show correctness of interaction.

1. Each server j verifies that for all $i \in \Lambda \setminus \{j\}$:

?

- $S_i^{V_1} \equiv (U_i^{-1} \prod_{v \in \Lambda} R_{i,v})^{V_2}$ where: $V_1 = \prod_{v \in \Lambda \setminus \{i\}} (1 +$

$$x_v) \text{ and } V_2 = \prod_{v \in \Lambda \setminus \{i\}} (x_i - x_v).$$

If the verification does not pass, then server i is removed and new Λ is chosen.

$$(14) \quad \bullet \quad |r_{i,j,0}| \leq n-1, \text{ and } g^{r_{i,j,0} \cdot L^2} g_1^{r'_{i,j,0}} \equiv R_{i,j}$$

If verifications are disputed by j then $r_{i,j,0}$ and $r'_{i,j,0}$ is revealed (decommitted), and either i or j is removed appropriately. Protocol is halted.

The first verification (on the magnitude of $r_{i,j,0}$) is used to prevent an attack in which the adversary sends very large values so that the shareholder can not compute efficiently. Different techniques can be used such as the size of packets (fields) which transmit $r_{i,j,0}$ may be of a fixed size but large enough.

2. If all verifications pass, shadowholder's $j \in \Lambda$ new shadow is $s'_j = -r''_j + \sum_{i \in \Lambda} r_{i,j,0}$ such that L divides s'_j and $0 \leq r''_j < L$.

3. Shareholder j publishes r''_j and $Q = \prod_{v \in \Lambda} g_1^{r'_{v,j,0}}$.

Note that any attempt to spoil the computations forces an adversarial server to be removed. When the protocol is used in an environment when $I \geq 2(t-1)+1$ servers, we can revise the set Λ to a new set of t shareholders and redo the set of shareholders from start.

Remark: splitting the shares in step 2 above is not necessary at this point, but will be used in the proactive extension discussed below.

A SECURE THRESHOLD RSA SCHEME

Discussed here is a secure threshold RSA protocol. As stated above in the section titled, "A Heuristic Threshold RSA Scheme," it is not known how to prove the security of the heuristic RSA threshold cryptosystem in the static adversary model. The problem is proving security when the subsets of signers change from message to message -- which makes its

(15)

security only a heuristic. To get a provably secure protocol, the approach is to dynamically convert the singing shares of the current set of t shareholders employing the poly to sum technique above. Then the signing is done using the shares of the sum. "Dynamically converting" here means that any new set of t shareholders have to go through the above poly to sum technique prior to singing. This will make partial views available to the adversary random and independent, and will permit one to "simulate" the adversary's view. By demonstrating that one can simulate the view, one can give a proof of security as follows.

Step 0 (Setup): The share distribution protocol of the section titled, "A Heuristic Threshold RSA Scheme" is performed, and encryption keys for each server are distributed. It is assumed that the dealer during setup publishes elements $g, g_1 \in \mathbb{Z}_n^*$ of maximal order where $g_1 = g^a$ for a relatively prime to $\theta(n)$, (the elements can be part of each server's key). $S_i = g^{s_i} L^2 \bmod n$ for all i is made public as well.

Step 1 (Poly to Sum): Perform the poly to sum (share-of-shares) protocol of the section above entitled "Share of Shares (Poly to Sum)" ("Poly to Sum") until a set of t servers which successfully complete the poly to sum protocol without disputes is found. Let Λ be the t servers which successfully completed the protocol.

Step 2 (Signing): To sign for each input message m , each server in Λ broadcasts partial result $S_{m,i,\Lambda} = m^{s_i} \bmod n$ where s_i is from "Poly to Sum." Observe that $m^d \equiv m^{P \cdot W} \cdot \prod_{i \in \Lambda} S_{m,i,\Lambda} \bmod n$, where $W = \sum_{i \in \Lambda} r_i$, which can be easily computed by the publicly available combining function. Shareholders in Λ can

(16)

now sign as many messages as they desire using the s' shares they obtained in the poly to sum protocol without performing the poly to sum conversion again. As a performance optimization note that a server can keep in its cache polynomially many shares for different Λ 's.

EMPLOYING A CHECKING PROTOCOL TO ASSURE ROBUSTNESS IN THE RESILIENT DISTRIBUTED CRYPTOGRAPHIC FUNCTION SERVER.

In the distributed cryptographic service, we may want to assure integrity of the partial results. To this end, the units may engage in a checking protocol between a unit and the output process. As a result of this protocol the output process can decide which partial result is correct and which to discard, i.e. it performs an error-detection and elimination process. Given the remaining correct partial results, the output process can combine and compute the final result.

As an alternative to error detection and elimination, the output process may apply an error correction procedure that computes with correct and incorrect pieces, but as long as there is a quorum of correct partial results, the final result is correct. This assures that the robustness is maintained even in a system where some components may fail (hardware or software failures). Note that input and output processes need to be replicated in high availability system in an environment where components may fail.

Fig. 8 illustrates a checking protocol for a robust cryptographic system. As depicted in the 3 out of 3 configuration, the three servers 421, 423, and 425 in combination with the combining function 427 are performing a protocol. (The combining function 427 may be shared in another server, such as 421, 423, 425 and/or other servers.) The verification protocol for 421's partial result is performed via the interactions 421 has with 423, 425 and 427

(17)

as depicted by 429. An exemplary verification for an RSA scheme is discussed below.

ROBUST THRESHOLD RSA SCHEME

The scheme described above in the section titled, "A Secure Threshold RSA Scheme," is secure but it is not robust. A subset of size t may include a misbehaving party during signing, and a new subset will have to be considered. Robustness provides for efficient verification of a shareholder's computation. The secure threshold RSA protocol can be made robust as discussed below.

Setup: Let Verifier be the entity that computes the efficient combining function to obtain $m^d \bmod n$ from the output of the shareholders. Let s_i be server i 's share generated from the share of share protocol in the section above titled, "Shares of Shares (Poly to Sum)," and let witness $S_i' \equiv g^{s_i} \cdot L^2 \equiv (\prod_{r \in A} R_{r,i}) \cdot (Q_i g^{r_i} L^2) \bmod n$ be generated using public information provided in "Shares of Shares (Poly to Sum)."

Verify partial result: One can use a technique from Y. Frankel, P. Gemmel and M. Yung, "Witness Based Cryptographic Program Checking and Robust Function Sharing," Proceedings of the 28th Annual Symposium on Theory of Computing, ACM, 1996, pp. 499-508 ("[FGY]"), or for super-safe prime RSA, one can use a technique from R. Genaro, S. Jarecki, H. Krawczyk, T. Rabin, "Robust Threshold RSA, Advances in Cryptology -- Crypto 96 Proceedings," Lecture Notes in Computer Science, Vol. 1109, N. Kobitz ed., Springer-Verlag, 1996, pp. 157-172, ("[GJKR2]"). There are known random elements (generators of subgroups) g_i and the result of the shareholder's function applied to them (which are called "witnesses"). For simplicity

(18)

of presentation one can assume one such generator g of a maximal order. (Alternatively, one may use a number of random generators that are exponentiated separately and then are multiplied together with the message to create a checker data.) The protocol goes as follows:

1. The Verifier gives to shadowholder i : the message m and checker $M = m^{q_0} g^{q_1} \bmod n$ for $q_0, q_1 \in_R \{0, \dots, n-1\}$.
2. The Verifier proves (e.g., in a two round protocol of [FGY]) that it knows the elements q_0, q_1 .
3. Shadowholder returns partial result $S_{m,i,\Lambda} = m^{S'_i} \bmod n$ and $H = M^{S'_i} \bmod n$.
4. Let $S'_{m,i,\Lambda}, H$ be received by Verifier. Then Verifier verifies that

$$(H')^{L^2 ?} \equiv (S'_{m,i,\Lambda})^{L^2 \cdot q_0} (S'_i)^{q_1} \bmod n. \quad \text{If the test}$$

fails, then an error is detected.

An implementation which is a combined protocol which comprises of initial setup of shares distributed with published witnesses. The protocol of the section above titled "A Secure Threshold RSA Protocol," running with "Verification of Partial Results" as above, is a "robust threshold RSA" which: (1) is optimal-resilience, and (2) has small permanent share size of the order of the size of the secret.

EMPLOYING A UNIT INTEGRITY FUNCTION WITHIN THE RESILIENT DISTRIBUTED CRYPTOGRAPHIC FUNCTION SERVER

Applications of the distributed cryptographic service of high resilience may be a sharing of a key by different organizations, with each organization holding a key share. Each organization may belong to a different country or

(19)

to a different business entity, which makes the unit mutually distrustful. Fig. 9 illustrates an arrangement for a shareholder that provides an additional layer of protection in consideration of non-trusting entities. Item 451 designates a shareholder as an organization, while items 453 and 455 designate equipment units used by the organization 451. A measure of distrust arises, for example, when the source that built and/or designed the secret share holding/computing unit 455 is not be entity 451. Therefore, there is a mutual distrust between the builder/designer of unit 455 and the user organization 451.

In this case each shareholder organization 451 entrusts its share to unit 455, but also relies on a second unit 453 whose task is assuring the integrity of unit 453. This unit-integrity unit 453 will work with the computing unit 455 to, e.g., (1) supply the computing unit 455 with random bits for computation, (2) engage in an "interactive checking protocol" to assure robustness and correctness of the result, and (3) prevent leakage of information out of the computing unit to the network 457. The integrity unit 453 will provide assurance not only that the correct output was presented by 455, but also that there are no subliminal channels, timing channels or other forms of covert channels. Other protection mechanisms may be enforced by the firewall as defined by policies. This provides a firewall protection for each of the units.

SMALL-SHARE ROBUST THRESHOLD RSA

Part of the reason that the above scheme has large shares is due to the need to have shares of a specific form to allow for proactivization. When proactivization is not needed, a secure threshold RSA scheme exists where shares are of the order of the RSA key. A "size efficient secure RSA

(20)

function sharing" exists where a permanent share is only a small constant times the secret's size.

To implement this, let $r(x)$ be as in the section above entitled "A heuristic threshold RSA scheme." Distribute shares as $s_i \equiv (r(i)/L) \bmod \theta(n)$ which is possible since L divides $r(i)$ in the integers. For the shares held after the poly to sum protocol, only $s_i s_j z_{i,j} / \gcd(L / \prod_{j \in \Lambda \setminus \{i\}} (x_i - x_j))$ must be stored and $\gcd(L, \prod_{j \in \Lambda \setminus \{i\}} (x_i - x_j))$ made publicly available to server.

All exponentiations are computed first with s_i' and then raised by $\gcd(L, \prod_{j \in \Lambda \setminus \{i\}} (x_i - x_j))$. Observe that the user must also possess a decryption key for the private computations.

SECURE PROACTIVE RSA

In order to protect against a mobile adversary, the shareholders reshuffle (re-randomize) their shares. If the adversary has access to the memory of a server at some point in time, and later the adversary is removed from the server, that past information is useless to the adversary after an update period. Figure 10 illustrates reshuffling in a distributed system. A system of 5 servers 361, 363, 365, 367 and 369 have shares $s_{i,j}$ which change as the time period changes. For instance, server 361 has share $s_{1,1}$ at time period 1, $s_{1,2}$ at time period 2, and $s_{1,3}$ at time period 3. The combining function 371 is not affected during the time periods but it is acceptable that a different server function as 371 within a single time period and between several time periods.

Discussed here is a secure proactive RSA protocol where in this variant of the implementation shares are refreshed.

(21)

SHARE DISTRIBUTION (SETUP): This is a setup as in the robust threshold RSA in the section "Robust Threshold RSA Scheme." The dealer generates an RSA with public key (e, n) and private key d . It then generates shares $s_{i,0}$ of $L \cdot K'$ as in the section titled "A Heuristic Threshold RSA Scheme." The dealer also publishes $\{g, g^d\}$ for a $g \in \mathbb{Z}_n^*$ of maximal order and for all i the value $g^{s_{i,0} \cdot L} \bmod n$ (if we employ more generators, it publishes this value with respect to each of them).

UPDATE PERIOD: Let $u \leftarrow u + 1$.

SHARE RENEWAL AND RECOVERY: The intent is to make shares at time $u + 1$ be t -wise independent of shares held at time u . A "poly to sum" share of shares protocol is performed to create a t -out-of- t sharing of $L \cdot K' = W + \sum_{i \in \Lambda} s_i'$ where W is a public value dividing L . Now the shares are additively shared, then subject to a "sum to poly" share of share operation. Namely, each server i shares its s_i' (and the resulting public value W as well) with all servers j using the Shamir threshold scheme. Each of the l shareholders now sums up all the poly shares of each of the t shadows s_i' , generated by Λ . Hence each shadow holder will have a share of $L \cdot k'$.

The protocol updates all user's shares. Hence, whether old shares exist (renewal) or do not exist (recovery) is irrelevant, since the newly dealt share becomes the mechanism by which signing is performed. The following is done:

1. Perform the "poly to sum" share of shares protocol (Section "Shares of Shares (Poly to Sum)") with shares from time $u - 1$, $s_{i,u-1}$, until a set of t shadowholders defined by Λ have no dispute and agree to shares their respective s_i' and the public W .
2. Perform the following "sum to poly" share of share protocol (the goal is to randomly re-share the value as the value of a polynomial in location $l + 1$):

(22)

- (a) Each $i \in \Lambda$ shares its s_i (the lowest numbered member also shares the public W in its share, i.e., $s_i \leftarrow s_i + W$ for smallest $i \in \Lambda$). The sharing is done by generating a random polynomial $r_i''(x)$ of degree $t - 1$ with coefficients in $\{0, L, \dots, LC\}$, where C is as in the section titled "A Heuristic Threshold RSA Scheme." and then computes $r_i'(x) = r_i''(x) - r_i''(I+1) + s_i = \sum_{v=0}^{t-1} a_{i,v} x^v$, a polynomial to share $r_i'(I+1) + s_i$ in which L divides all shares.
- (b) Server $i \in \Lambda$ then publishes all the $g^{a_{i,v} \cdot L^2}$ and privately transmits $w_{i,j} = r_i'(j) \in \mathbb{Z}$ for $j \in \{1, \dots, J\}$.
- (c) Each server j verifies:
- Similar to [F] verify (proper share):

$$g^{w_{i,j} \cdot L^2} \stackrel{?}{=} \prod_{v=0}^{t-1} (g^{a_{i,v}})^{L^2 j^v} \pmod{n}$$
 - verify (proper secret): $g^{s_i} L^2$

$$\stackrel{?}{=} \prod_{v=0}^{t-1} (g^{a_{i,v}})^{L^2 (I+1)^v} \pmod{n}, \text{ where witness}$$

$$g^{s_i} \cdot L^2 \equiv \prod_{j \in \Lambda} R_{j,j} \pmod{n}$$
 is generated from public values in Section "Shares of Shares (poly to sum)", (except for the server with lowest index which must multiply by $g^{W \cdot L^2}$).
 - verify correct form: L divides $w_{i,j}$
- (d) Then dispute resolution is performed. Detected faulty and corrupted system components (servers) are

(23)

rebooted and the share renewal process continues from the beginning until there are no disputes.

(e) Now $s_{i,u} = \sum_{j \in \Lambda} w_{j,i}$. Erase previous history and retain new current shadow $s_{i,u}$. The $g^{s_{i,u} \cdot L^2}$ are published using the multiplication mod n of $g^{L^2 \cdot w_{i,j}}$.

3. The common "public" constants (such as the system size l , the public part of the key P , and the value of the generators) that are maintained proactively by a simple memory "refresh" procedure: each server sends to each server its current value and then the majority value becomes the new permanent value.

The size of the $w_{i,j}$ is sent via packets (fields) which are of fixed size large enough in order to prevent an attack in which the adversary sends such large shares that the shareholder can not compute with efficiently.

RSA FUNCTION APPLICATION: Let time be u . Performed exactly as the secure threshold RSA in Section entitled "A secure threshold RSA scheme" with shadow $s_{i,u}$ if robustness is not required, otherwise perform the computation with verification as in the protocol of the section entitled "Robust Threshold RSA Scheme."

Dynamic Management Function Sharing

The embodiment can serve other purposes. The above method is a very flexible transformation going from t -out-of- l to additive sharing t -out-of- t and back. One can, when going back, change the sharing threshold and increase the number of servers and have, say t' -out-of- l' (assuming, of course that at most $t' - 1$ if $t' < t$ can be corrupted at the update). Also, one can decrease the number of servers in a similar way

(24)

and under analogous assumptions about corrupted servers. This demonstrates the strength of this flexible technique.

The system can change in multiple ways with respect to dynamic management: no change, add user/same threshold, add user/decrease threshold, add user/increase threshold, delete user/same threshold, delete user/decrease threshold and delete user/increase threshold. Figure 11 illustrates a distributed system having changes in the number of users and threshold. In a system initially consisting of a 3 out of 5 system with servers 401, 403, 405, 407 and 409, an "add user/increase threshold dynamic management" operation is performed to include server 411. After the "add user/increase threshold dynamic management" operation, the system is a 4 out of 6 system. As also depicted Fig. 11, if the delete user/same threshold dynamic management system is performed server 409 is removed and the system becomes a 4 out of 5 system.

A Note: against an adversary that is only curious but does not affect memories of servers, namely it is not disruptive (malicious), one can have polynomial of larger degrees t even when $t > n/2$ when one is sure that t servers are always available (since the adversary only reads memories), and the adversary can control at most $t - 1$ of them at any period.

3.9 A Generalized Embodiment of Proactive System

Fig. 12 illustrates the notion of sharing of a general homomorphic function. The function F depicted as 421 accepts as input a message M and a secret key k , then given these two input values, returns result $F_k(M)$. The pro-active system re-expresses 421 (which is keyed with the secret k) by introducing servers 423, 425, 427, 429, 431 and 433. The illustrated system is a 3 out of 5 system, in which any 3 of the servers chosen from 423, 425, 427, 429 and 431 can work together with 433 in order to generate the value $F_k(m)$ in a distributed fashion.

(25)

Discussed below is a generalization of the previous embodiment from an RSA system to a generalized set of functions which are called trapdoor permutation. A trapdoor permutation family were introduced by W. Diffie, and M. Hellman, *New Directions in Cryptography*, *IEEE Trans. on Information Theory*, 22 (6), 1976 ("[DH]") and are discussed below.

Definition 1: A trapdoor permutation family \mathcal{T}_h consists of a polynomial time generator G that, when given an input 1^h (h the security parameter) returns (WLOG) a randomly drawn tuple consisting of two h bit strings (pu, se) where pu is a public key and se is the secret key. The keys define permutations, $f_{pu}(\cdot)$ and $f_{se}(\cdot)$, over the sample-able message space \mathcal{D}_{pu} such that $f_{se}(\cdot)$ is the inverse function for $f_{pu}(\cdot)$ and given $pu(se)$ applying $f_{pu}(\cdot)(f_{se}(\cdot))$ is polynomial time.

Finding inverses of random values of a randomly chosen permutation without having the secret key se is hard. That is, for all probabilistic polynomial time algorithms A , for any polynomial $\text{poly}(\cdot)$, for all h large enough:

$$P[f_{pu}(u) = w : (pu, se) \leftarrow G(1^h); w \in_R \{0, 1\}^h; u \leftarrow A(1^h, pu, w)] < \frac{1}{\text{poly}(h)}.$$

Recall that, $P[x:e_1; \dots, e_j]$ is the standard notation for the probability of predicated x after the events e_i occur (are executed) sequentially.

SUFFICIENT CONDITIONS

The following are sufficient conditions for the permutation. The notion of share-translation condition below provides sufficient algebraic properties to assure that a function is share-able.

(26)

Definition 2 (Share-Translation): Let the secret key be $se = k$. A trapdoor (hard to compute) permutation $f_k(\cdot)$ is share-translate-able when: 1) there exists an Abelian share space group $\mathcal{K}_{se}(+)$ where $k \in \mathcal{K}_{se}$, 2) there exists a polynomial time "mapping" $f : \mathcal{K}_{se} \times \mathcal{D}_{pu} \rightarrow \mathcal{D}_{pu}$ such that $f'_k = f_k$, 3) the probability that f is not defined for one or more randomly chosen $\text{poly}(h)$ elements in \mathcal{D}_{pu} is negligible, and 4) there exists an associated binary operation "+" for the set \mathcal{D}_{pu} such that $f'_{k_1}(\alpha) * f'_{k_2}(\alpha) = f'_{k_1+k_2}(\alpha)$ for any $k_1, k_2 \in \mathcal{K}_{se}$ and a $\alpha \in \mathcal{D}_{pu}$.

A family of trapdoor permutations \mathcal{F}_h is "share-translate-able" if almost all elements in it are share-translate-able." A sufficient condition such that all of the operations in a function sharing primitive are computable in polynomial time in the security parameter was defined in A De Santis, Y. Desmedt, Y. Frankel, and M. Yung, *How to Share a Function Securely*, ACM Proceedings of the 26th Annual Symposium on Theory of Computing, ACM, 1994, pp. 522-533 ("DDFY"), and can be stated as follows.

Definition 3 (Share Efficiency) A trapdoor permutation is efficiently (polynomial time) share-translate-able when 1) given pu , multiplying elements and computing inverses in the message space \mathcal{D}_{pu} is polynomial time in h , 2) share space \mathcal{K}_{se} is a sample-able set, 3) the share space $\mathcal{K}_{se}(+)$ is an Abelian group such that given se one can perform the "+" and inverses in polynomial time in h , and 4) \mathcal{K}_{se} may be found in probabilistic polynomial time, given se .

A family of trapdoor permutations \mathcal{F}_h is efficiently share-translate-able if almost every element in it is.

Share translation and share efficiency do not, on their own, guarantee security. For the function sharing protocol to be secure, all of the information the adversary

(27)

receives must not allow it to break the system. To provide for security, all the information that the adversary would receive is simulate-able given public information.

The share space is often not sample-able as, for instance, the RSA function where the share space of the trapdoor permutation could be $\mathcal{K}_{se} = Z_{\phi(n)}(+)$. Leaking any information about $\phi(n)$ may compromise security. Picking a random number in $\{0, \dots, \phi(n)-1\}$ can be simulated by $\mathcal{D}_{pu} = \{0, \dots, n-1\}$ using only public information in order to provide a means in which to simulate share distribution.

The simulate-able property states that given public information only, one can, in polynomial time, simulate the actions of g (the shared function) and \mathcal{K}_{se} via a function z (the simulate-able function) and Z_{pu} (the simulate-able share space) respectively. This can be stated as follows.

Definition 4 (Simulate-able) Let $(pu, se) \in \mathcal{F}_h$ be the input to a function sharing primitive. We say that the shadow function generation phase is simulate-able for \mathcal{F}_h when: 1) there exists a probabilistic polynomial time algorithm S_1 which, when given pu , returns a polynomial space description of Z_{pu} (defined below) and a polynomial time algorithm $z: Z_{pu} \times \mathcal{D}_{pu} \rightarrow \mathcal{D}_{pu}$, 2) there exists a probabilistic polynomial time algorithm S_2 :

$\{0,1\}^b \times \{0,1\}^b \times \mathcal{K}_{se} \rightarrow Z_{pu}$, such that $f'_k = z_k$ for

$k \leftarrow S_2(pu, se, k')$, and 3) distributions $\{x | x \in_R Z_{pu}\}$ and $\{x | y \in_R \mathcal{K}_{se}; x \leftarrow S_2(pu, se, y)\}$ are statistically indistinguishable.

A family of trapdoor permutations \mathcal{F}_h is simulate-able if almost every element in it is.

EXTENSIONS OF THE KEY SPACE

(28)

Discussed below is a definition of the extensions of the key space and how operations are performed on this key space.

Definition 5 (Key Space Extension) Let $Z[u]$ be an algebraic extension over the integers of degree m . The extended share space is the module $\mathcal{K}^{q-1} = \mathcal{K}_{ss} \times \cdots \times \mathcal{K}_{ss}$ (i.e., the direct product of m copies of \mathcal{K}_{ss}) over $Z[u]$.

One can create an extension of \mathcal{K}_{ss} which has the appropriate algebraic structure to perform Lagrange interpolation over any finite Abelian group uniformly for any I . Let q be a prime greater than or equal to $I + 1$ and u be a root of the cyclotomic polynomial $p(x) = (x^q - 1)/(x - 1) = \sum_{j=0}^{q-1} x^j$. This defines an extended key space $\mathcal{K}^{q-1} = \mathcal{K}_{ss} \times \cdots \times \mathcal{K}_{ss} \cong \mathcal{K}_{ss}[\mathbf{x}]/(\mathbf{p}(\mathbf{x}))$, the direct product of $q - 1$ copies of \mathcal{K}_{ss} . We consider \mathcal{K}^{q-1} as a module over $Z[u] \cong Z[\mathbf{x}]/(\mathbf{p}(\mathbf{x}))$ (i.e., the extension of integers with the element u).

Lemma 1: Let q be a prime greater than or equal to $I + 1$, and u be a root of the cyclotomic polynomial $p(x) = (x^q - 1)/(x - 1) = \sum_{j=0}^{q-1} x^j$. Let $\mathbf{x}_i = \sum_{j=0}^{i-1} u^j$. Then $(x_i - x_j)^{-1}$ exists for $0 \leq i \leq I$.

Proof. Using the extended Euclidean algorithm [HW] $(\mathbf{x}_i)^{-1}$, $1 \leq i \leq I$ is computed since $\gcd((u^q - 1)/(u - 1), (u^i - 1)/(u - 1)) = (u^{\gcd(q, i)} - 1)/(u - 1) = 1$ in $Z[u]$, $u - 1 \mid u^i - 1$, and q is a prime. Moreover, $\gcd(u^q - 1, u^i) = 1$. From this it is easy to see that $(\mathbf{x}_i - \mathbf{x}_j) = -|q|_0 u^{q_1} ((u^{q-2} - 1)/(u - 1))$, for some q_1 , has an inverse for $0 \leq i \leq I$. Therefore, this module has a scalar in which the \mathbf{x}_i and $\mathbf{x}_i - \mathbf{x}_j (i \neq j)$ have inverses when $X_v = (u^v - 1)/(u - 1) = \sum_{v'=0}^{v-1} u^{v'}$. This property is useful in creating a threshold scheme over this module.

(29)

Observe that $(u')^{-1} = u'^{-1}$. One can write elements $\mathcal{Z}^{q^{-1}}$ as $[k_0, \dots, k_{q-2}]$ and the identity element as $[0, \dots, 0]$, where 0 is the identity element of $\mathcal{Z}_{p^q}(+)$. Addition in $\mathcal{Z}^{q^{-1}}(+)$ is defined as $[k_0, \dots, k_{q-2}] + [k'_0, \dots, k'_{q-2}] = [k_0 + k'_0, \dots, k_{q-2} + k'_{q-2}]$. The scalar operation $(b_0 + \dots + b_{q-2} u'^{-2}) \cdot [k_0, \dots, k_{q-2}]$ is defined recursively from $b \cdot [k_0, \dots, k_{q-2}] = [b \cdot k_0, \dots, b \cdot k_{q-2}]$ for $b \in \mathbb{Z}$ and $u \cdot [k_0, \dots, k_{q-2}] = [0, k_0, \dots, k_{q-3}] + [-k_{q-2}, \dots, -k_{q-2}]$.

Definition 6 (Public Domain Extension) Let $\mathbb{Z}[u]$ be an algebraic extension over the integers of degree m . The extended public domain is the module $\mathcal{D}^{q^{-1}} = \mathcal{D}_{pu} \times \dots \times \mathcal{D}_{pu}$ (i.e., the direct product of m copies of \mathcal{D}_{pu}) over $\mathbb{Z}[u]$.

WLOG, one can assume the public domain is multiplicative. Similarly one can write elements $\mathcal{D}^{q^{-1}}$ as $[m_0, \dots, m_{q-2}]$ and the identity element as $[1, \dots, 1]$, where 1 is the identity element of $\mathcal{D}_{pu}(*)$. Multiplication in $\mathcal{D}^{q^{-1}}(*)$ is defined as $[m_0, \dots, m_{q-2}] * [m'_0, \dots, m'_{q-2}] = [m_0 \cdot m'_0, \dots, m_{q-2} \cdot m'_{q-2}]$. The scalar operation $[m_0, \dots, m_{q-2}]^{(b_0 + \dots + b_{q-2} u'^{-2})}$ is defined recursively from $[m_0, \dots, m_{q-2}]^b = [m_0^b, \dots, m_{q-2}^b]$ for $b \in \mathbb{Z}$ and $[m_0, \dots, m_{q-2}]^u = [1, m_0, \dots, m_{q-3}] * [m_{q-2}^{-1}, \dots, m_{q-2}^{-1}]$.

The DDFY Threshold Cryptosystem

Based on the theoretical basis set forth above, a general protocol can be implemented as follows. It will be appreciated that many variations in the manner of the use of algebraic extensions are possible and that similar techniques as with the use of finite geometry are also possible. For instance, extension over the integers in which there exists sufficient interpolation points x_i such that x_i and x_j , $x_i \neq x_j$, have inverses in the integer extension for all necessary interpolation points are usable.

(30)

Setup: Let $f_k(\cdot)$ be the function to be shared. Let $q > 1$ be a prime and u be a root of the cyclotomic polynomial $p(x) =$

$$\sum_{j=0}^{q-1} x^j. \text{ Let } \mathbf{x}_i = \sum_{j=0}^{q-1} u^j.$$

Share distribution phase: A random "polynomial" $r(x) =$

$$\sum_{v=0}^{q-1} a_v x^v \in$$

$\mathcal{R}^{q-1}[\mathbf{x}]$ is chosen such that $r([0, \dots, 0]) = [k, 0, \dots, 0]$ and

otherwise is random. It computes $s_i = [c_{i,0}, \dots, c_{i,q-2}] = r(\mathbf{x}_i)$.

It then publishes $(z^{-1}, z_{pu}) \leftarrow S_1(pu)$ and i 's private share is $s_i = [c_{i,0}, \dots, c_{i,q-2}]$ where $c_{i,j} = S_2(pu, se, c_{i,j})$.

Shared function evaluation phase: To jointly sign for a message m , server i transmits partial results, $S_{m,i} =$

$[m, 1, \dots, 1]^{s_i} \in \mathcal{D}^{q-1}$ to the combining function. Then the combining function calculates:

$$y_{i,\Lambda} = \prod_{\substack{v \in \Lambda \\ v \neq i}} (\mathbf{x}_i - \mathbf{x}_v)^{-1} (0 - \mathbf{x}_v).$$

(2)

and computes result $[f_k(m), \diamond, \dots, \diamond] = \prod_{i \in \Lambda} (S_{m,i})^{y_{i,\Lambda}}$ where \diamond represents an element in \mathcal{D}_{pu} which is not relevant.

For a function which satisfies Definitions 2, 3, and 4, the above is a secure and correct function sharing protocol. A. De Santis, Y. Desmedt, Y. Frankel and M. Yung, *How to Share a Function Securely*, ACM Proceedings of the 26th Annual symposium on Theory of Computing, ACM 1994, pp. 522-533.

The advantage of this is that this protocol is completely non-interactive. The shadow-holders never need to communicate with each other, directly or indirectly. This is due to the fact that a shadowholder does not need to know the identity of the shadowholders which it will do the distributed function sharing operation with. In practice, this may be very beneficial.

(31)

PRO-ACTIVIZATION

Discussed below is a method by which the protocol is proactivized as the preferred embodiment for generalized functions, beginning with the simulatability condition.

Definition 7 (Additive simulate-ability): Let Z'_{pu} be the set of integers which contains Z_{pu} . Moreover, there exists a polynomial time (in the length) predicate called Mem such that $\text{Mem}(a) = \text{TRUE}$ if and only if $a \in Z_{pu}$.

NOTE: it should be noted that Z_{pu} and Z'_{pu} (as denoted by pu) are different than Z_n the intergers modulo n .

The proactivization technique is to use the function application as above except that the update phase the poly to sum (see the section entitled "Shares of Shares (Poly to Sum)" above) is followed by the sum to poly phase (see "Secure Proactive RSA" above). For robustness one can use techniques analogous to the ones used for RSA based on Y. Frankel, P. Gemmell, P. Mackenzie and M. Yung, *Witness Based Cryptographic Program Checking and Robust Function Sharing*, *Proceedings of the 28th Annual Symposium on Theory of Computing ("[FGY]")*.

Definition 8 (Simulate-able Space Extension) Let $Z[u]$ be an algebraic extension over the integers of degree m . The extended public domain is the set with binary operation $Z^{q-1}(+) = Z'_{pu} \times \dots \times Z'_{pu}$ (i.e., the direct product of m copies of Z'_{pu} over $Z[u]$).

WLOG, one can assume the simulate-able space is additive. Similarly one can write elements Z^{q-1} as $\{s_0, \dots, s_q\}$.

(32)

$_2]$. Addition in $Z^{q-1}(+)$ is defined as $[s_0, \dots, s_{q-2}] + [s'_0, \dots, s'_{q-2}]$
 $= [s_0 + s'_0, \dots, s_{q-2} + s'_{q-2}]$. The scalar operation $(b_0 + \dots + b_{q-2} u^{q-2})$
 $^2 [s_0, \dots, s_{q-2}]$ is defined recursively from $b \cdot [s_0, \dots, s_{q-2}] =$
 $[b \cdot s_0, \dots, b \cdot s_{q-2}]$ for $b \in Z$ and $u \cdot [s_0, \dots, s_{q-2}] = [0, s_0, \dots, s_{q-3}] +$
 $[-s_{q-2}, \dots, -s_{q-2}]$.

OTHER FUNCTIONS

Proactive cryptosystems can also be based on cryptographic functions using discrete logarithms, including those defined over a composite. Hence for instance, El Gamal encryption can have an optimal resilience proactive system. RSA based variants such as elliptic curve RSA also have sufficient algebraic properties to be made proactive in accordance with the present invention.

POLY TO SUM WITH DDFY

Discussed below is a poly to sum method for the proactivization based on [DDFY].. Define selection function

σ , as $\sigma_i([s'_0, \dots, s'_{q-2}]) = s'_i$.

Setup: Assume that the dealer during share distribution publishes an element $g = [g', 1, \dots, 1]$ such that $g' \in \mathcal{D}_{pu}$ is of maximal order and it publishes $S_i = g^{s_i}$ for all i . Let Λ where $|\Lambda| = t$ be the shareholders (servers) participating in the share of shares protocol.

Sharing Shares: Server i .

- Generates $r_{i,j} \in_R Z_{pu}$

(33)

- Privately, transmit using probabilistic encryption over the public channel (an act which also publicly commits to the message) $r_{i,j}$ to server j .
- Sets the self-held share to be $r_{i,i} = \sigma_o(y_{i,\Lambda} \cdot s_i) - \sum_{j \in \Lambda \setminus \{i\}} r_{i,j} \in \mathbb{Z}_{pu}$, ($y_{i,\Lambda}$ as in equation (2)).
- Publish $R_{i,j} = g^{r_{i,j}}$.

Verify and generate shares: Let $r_{i,j}$ be the share received by j from i .

1. Each server j verifies that for all $i \in \Lambda \setminus \{j\}$:

$$\bullet \quad (S_i)^{V_1} \stackrel{?}{=} \prod_{v \in \Lambda} (R_{i,v})^{V_2} \text{ where } V_1 = \prod_{v \in \Lambda \setminus \{i\}} (0 - x_v)$$

$$\text{and } V_2 = \prod_{v \in \Lambda \setminus \{i\}} (x_i - x_v).$$

If the verification does not pass then server i is removed and new Λ is chosen.

$$\bullet \quad \text{for } i \neq j, \text{ Mem}(r_{i,j}) \stackrel{?}{=} \text{True and } g^{r_{i,j}} \stackrel{?}{=} R_{i,j}$$

If verifications are disputed by j , then $r_{i,j}$ is revealed (decommitted), and either i or j is removed appropriately. The protocol is halted.

2. If all verifications pass, shadowholder's j new shadow is $s'_j = \sum_{i \in \Lambda} r_{i,j}$.

THE PROACTIVIZED DDFY PROTOCOL

Share distribution (setup) Let $U = 0$.

(34)

Let $k \in \mathcal{K}_{ss}$ be the secret and let $f_k(\cdot)$ be the function to be shared. Let $q > 1$ be a prime, u be a root of the cyclotomic polynomial $p(x) = \sum_{j=0}^{q-1} x^j$ and $x_i = \sum_{j=0}^{q-1} u^j$.

The dealer chooses a random "polynomial" $r(x) = \sum_{i=0}^{q-1} a_i x^i \in \mathcal{R}^{q-1}[x]$ such that $r(\{0, \dots, 0\}) = [k, 0, \dots, 0]$ and otherwise is random. It computes $s_i' = [c_{i,0}', \dots, c_{i,q-2}'] = r(x_i)$. It publishes $(x^{-1}, Z_{pu}) \leftarrow S_1(pu)$ and privately transmits to server i share $s_i = [c_{i,0}, \dots, c_{i,q-2}]$ where $s_i' = [c_{i,0}', \dots, c_{i,q-2}']$ and $c_{i,j} = S_2(pu, se, c_{i,j}')$. The dealer publishes an element $g = [g', 1, \dots, 1]$ such that $g' \in \mathcal{D}_{pu}$ is of maximal order and it publishes $S_i = g^{s_i}$ for all i .

Update period: Let $U \leftarrow U + 1$.

1. Perform the "poly to sum" share of shares protocol (Section entitled "Poly to Sum with DDFY") with shares from time $U-1$, $s_{i,U-1}$, until a set of t shadowholders defined by Λ have no dispute and agree to shares their respective s_i' .
2. Perform the "sum to poly" share of share protocol:
 - (a) Each $I \in \Lambda$ shares its s_i' by generating a random polynomial $r_i'(x) = s_i' + \sum_{r=1}^{t-1} a_{i,r} x^r$ of degree $t = 1$ with coefficients $a_{i,r} \in \mathcal{R}Z^{q-1}$.
 - (b) Server $j \in \Lambda$ then publishes all the $g^{a_{i,r}}$ and privately transmits $w_{i,j} = r_i'(x_j)$ for $j \in \{1, \dots, t\}$.
 - (c) Each server j verifies:
 - Similar to [F] verify:

(35)

$$g^{w_{i,j}} \stackrel{?}{=} g^{s_i} \prod_{r=1}^{t-1} g^{s_{i,v}^{(x_j)^v}} \quad \text{where witness}$$

$g^{s_i} \equiv \prod_{j \in \Lambda} R_{j,i}$ is generated from public values i (Section entitled "Shares of Shares (Poly to Sum)").

- (d) Then dispute resolution is performed. Detected faulty and corrupted systems are rebooted and the share renewal process continues from the beginning until there are not disputes.

- (e) Now $s_{i,u} = \sum_{j \in \Lambda} w_{j,i}$. Erase previous history and retain new current shadow $s_{i,u}$. The $g^{s_{i,u}}$ are computed using the $g^{w_{i,j}}$.

The size of the $w_{i,j}$ is sent via packets (fields) which are of fixed size large enough in order to prevent an attack in which the adversary sends such large shares that the shareholder can not compute with efficiently.

Shared function application: Let time be U . Performed as the [DDFY] scheme as presented in the section titled "The DDFY Threshold Cryptosystem") with shadow $s_{i,u}$ except that servers keys are in $Z_{pu}^1 \times \dots \times Z_{pu}^1$ rather than $Z_{pu} \times \dots \times Z_{pu}$. For robustness, use [FGY] protocol using witness $g^{s_{i,u}}$.

The embodiments described herein use relatively efficient constructions that are based on servers evaluating and transmitting cryptographic functions' values. The techniques of the present invention can also be applied to less efficient communication constructions characterized by the theoretical notion of "secure circuit evaluation," where

(36)

the theoretical notion of "secure circuit evaluation," where the communication is proportional to the size of circuits computing the cryptographic functions.

Another application of the "proactive model" is a flexible key management of shareholders in a function sharing scheme. It enables to change the set of shareholders during the refreshing period by giving the recovered new share to a new server, rather than the old one. The protocols of the present invention extend this capability, and enable dynamic changes of the threshold value as well.

The previous discussion addressed certain "size parameters" (e.g., length of keys and of shares of keys etc.). It is contemplated that one would choose size, or relative size, of keys according to a notion of "security level" and its tradeoff against "performance level." For increased security one would choose a longer set of keys, and a longer key takes more memory space and more computation time to calculate. The size parameters can be varied as a system's parameter providing higher security when increased, or higher performance when decreased.

Other examples of applications of the present invention include: 1) as a certification authority where the distributed system is used to produce certificates based on authorized inputs, and 2) as an escrow agency in which shareholders are escrow agents, and a plurality of escrow agents are needed to create a decryption of authorized cyphertext to be taken off escrow.

The embodiments described herein are intended to be illustrative and not limiting. It will be appreciated that many variations are possible within the scope and spirit of the invention.

(37)

We claim:

1. A method for performing computations on an input to generate an output, said computation defined by a particular instance of first function family, the method comprising the steps of:

reexpressing the instance of the first function family as a first plurality of instances of alternative function families;

at each of a plurality of distinct locations, applying an instance the alternative function family to the input to generate a plurality of partial result;

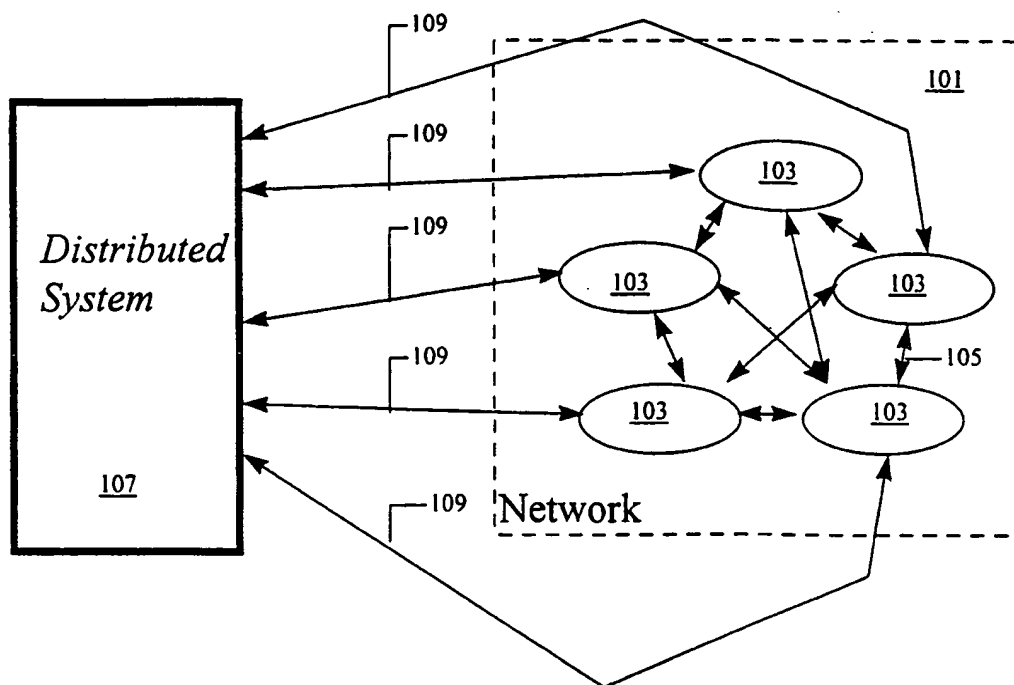
combining the partial results to obtain a final result;

wherein the final result is the same result as would be obtained by applying the instance fo the first function family to the input; and

reexpressing the instance of the first function family as a second plurality of instances of alternative function families and applying the second plurality of instances to inputs, such that

(1) at differing times, a location applies instances of differing function families, and

(2) combining partial results of applying each of the second plurality of instances of the alternative function families to the input produces a result that is the same as would be obtained by applying the instance of the first function family to the same input.

*Figure 1*

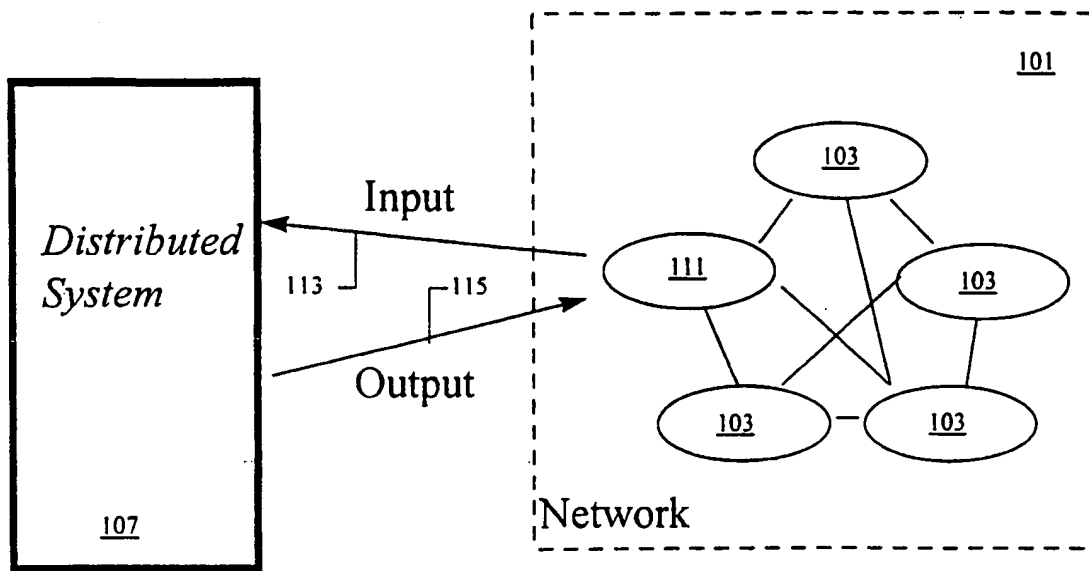


Figure 2

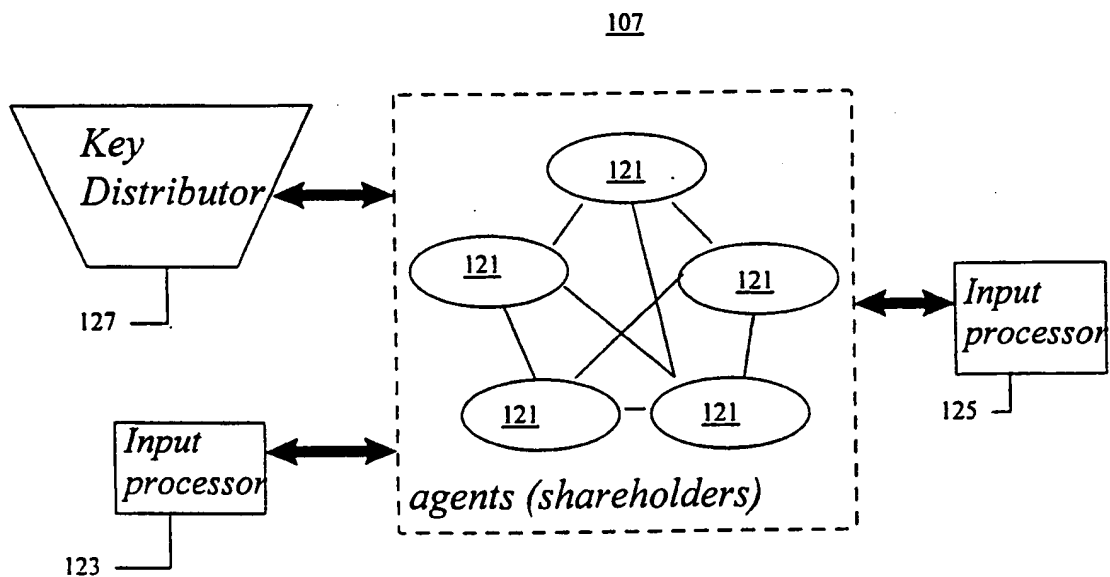
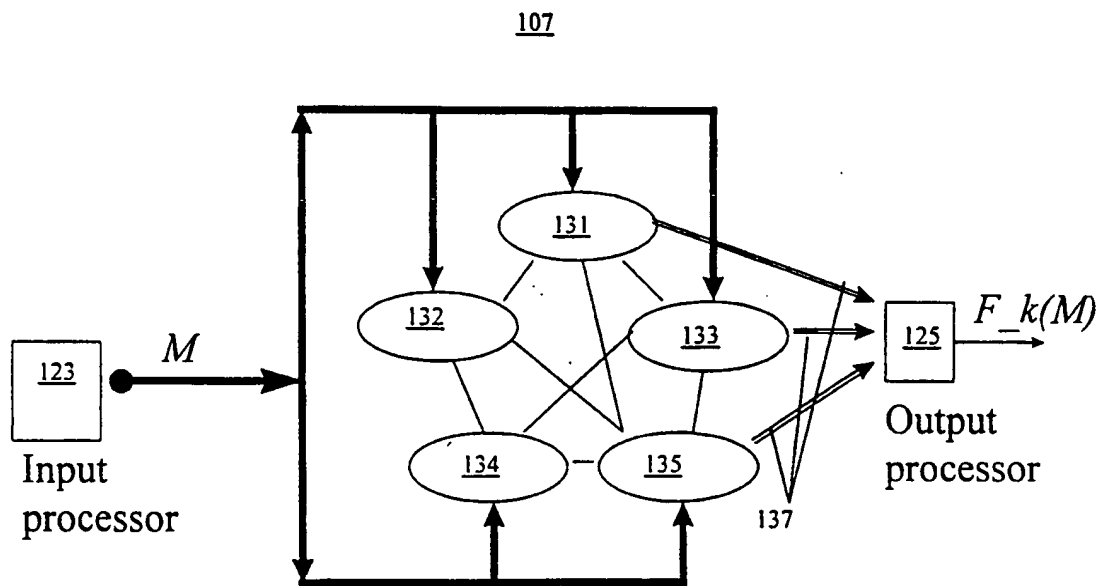


Figure 3

*Figure 4*

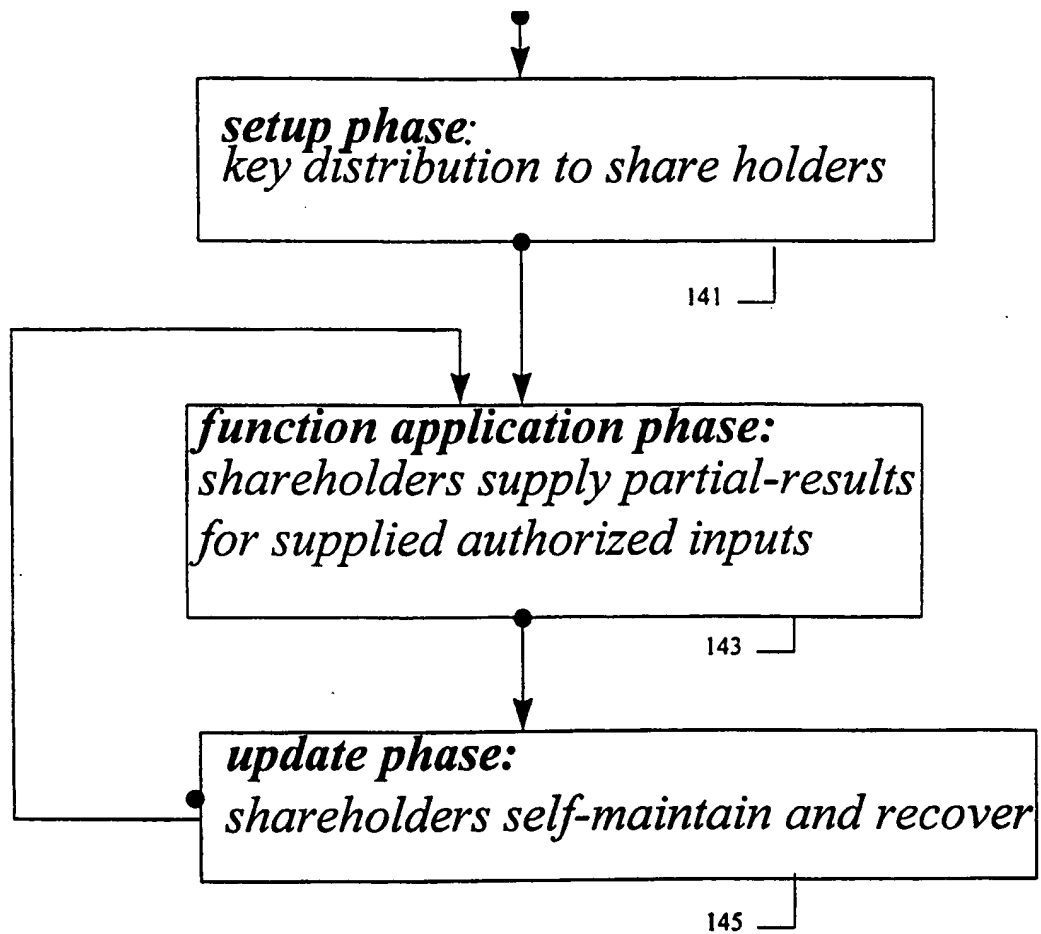
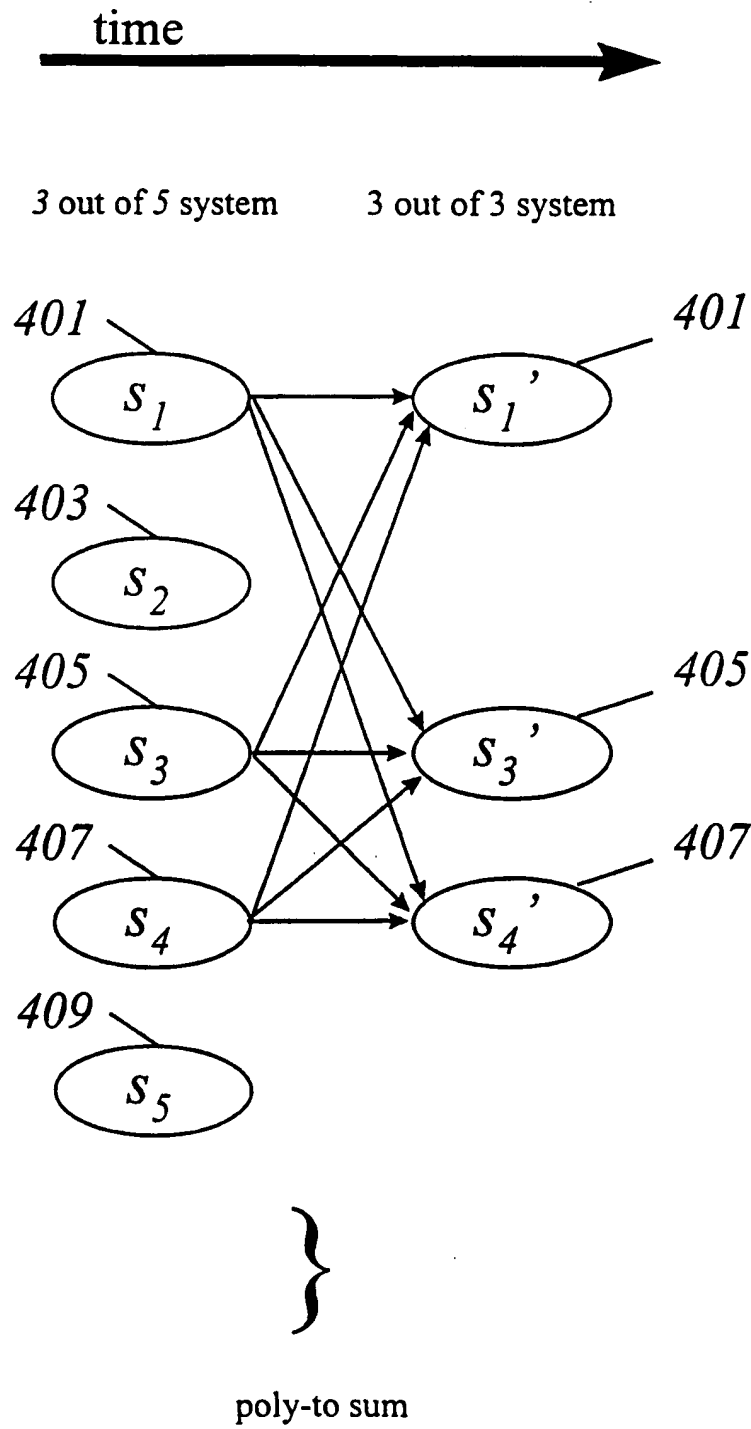


Figure 5

*Figure 6*

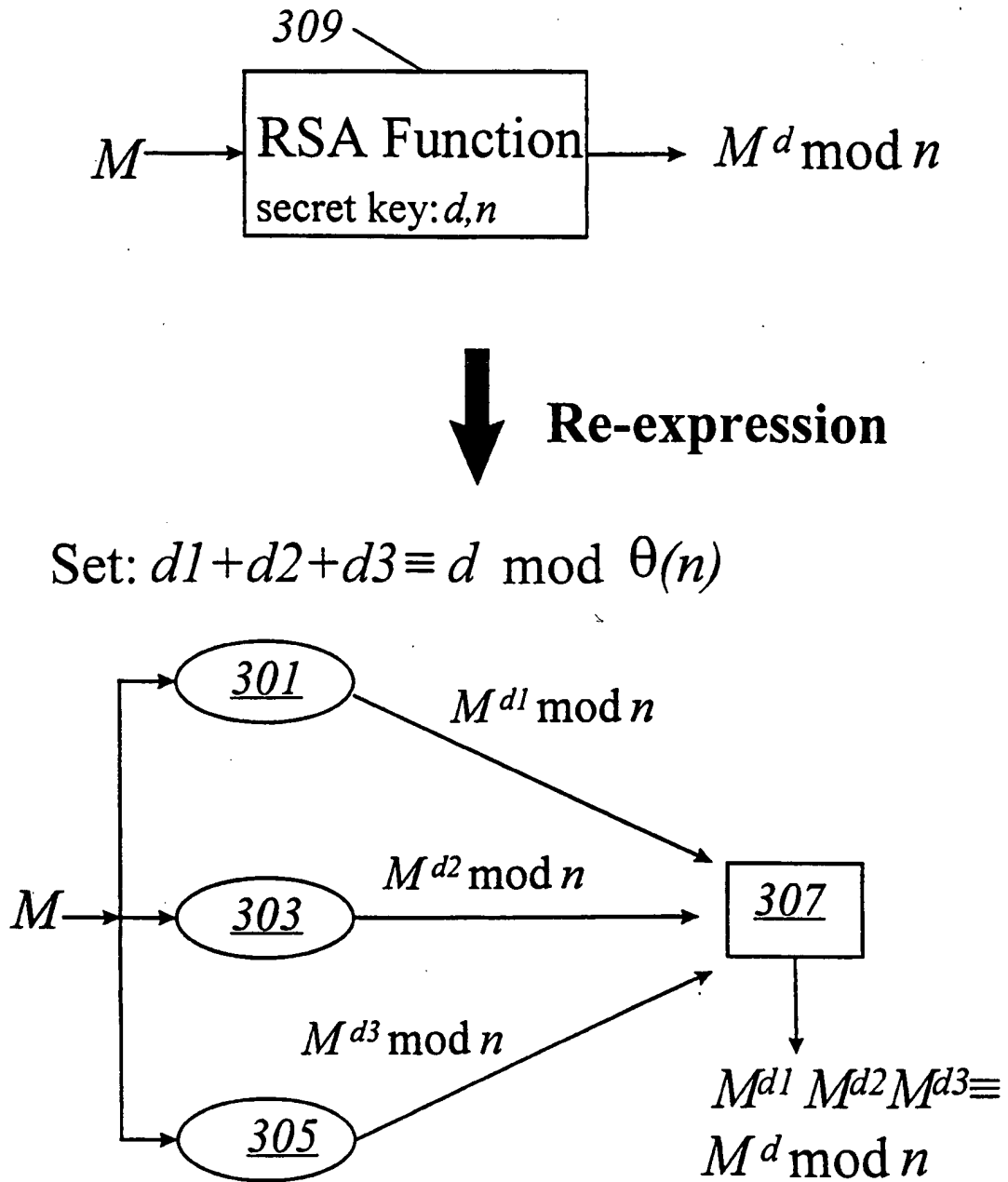


Figure 7

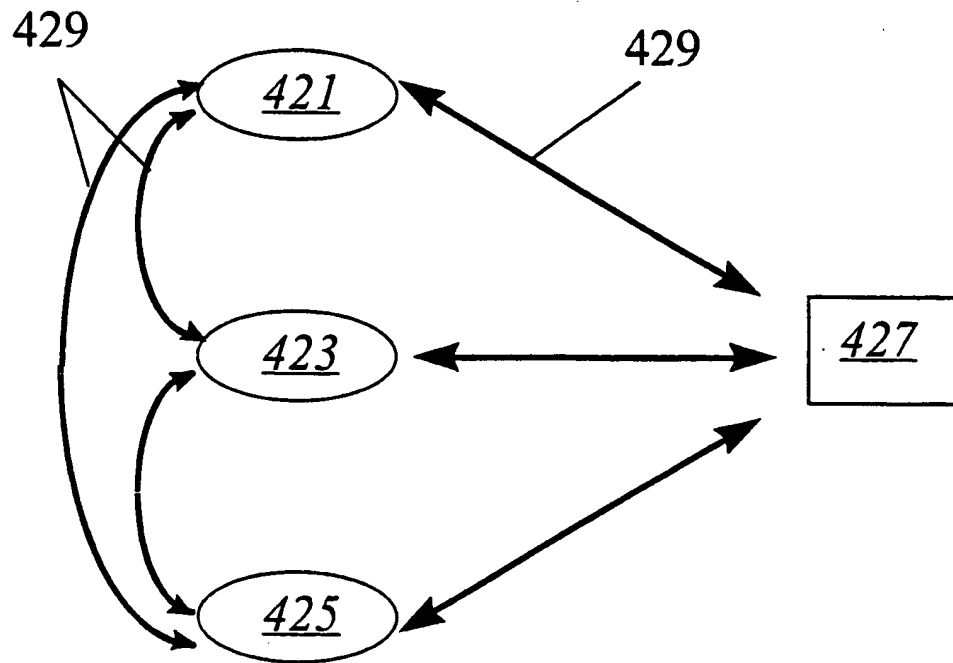


Figure 8

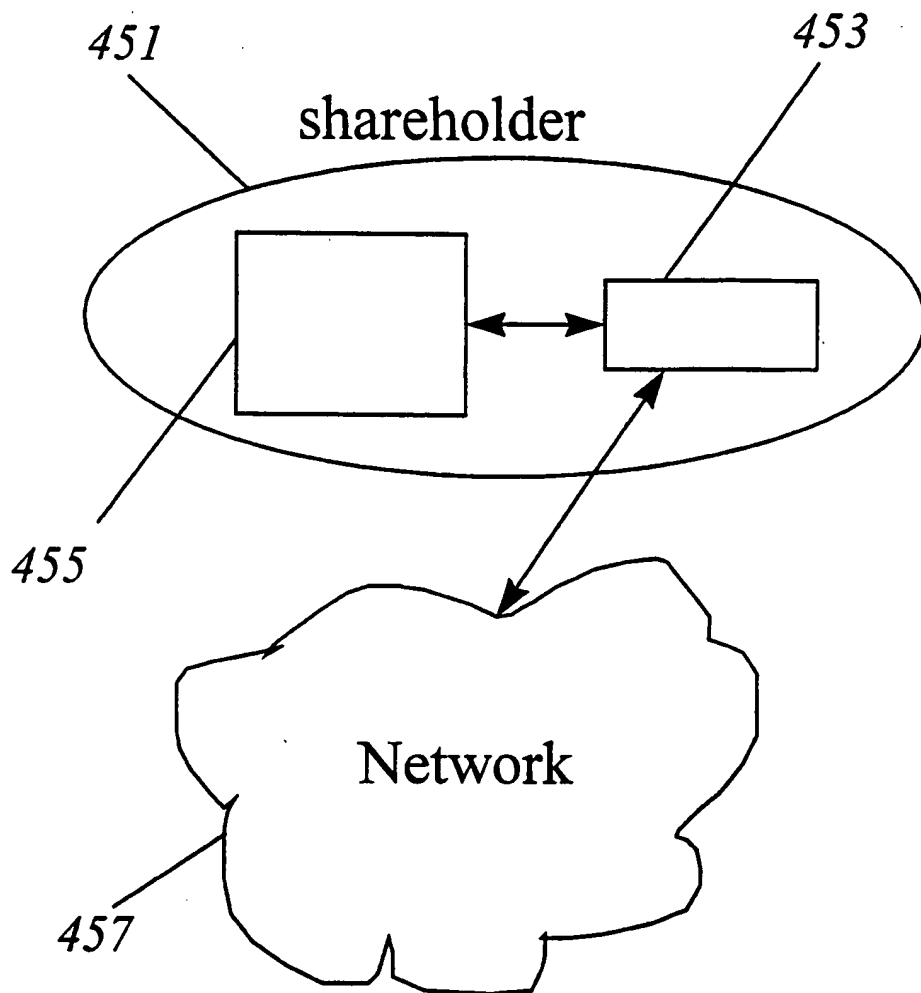


Figure 9

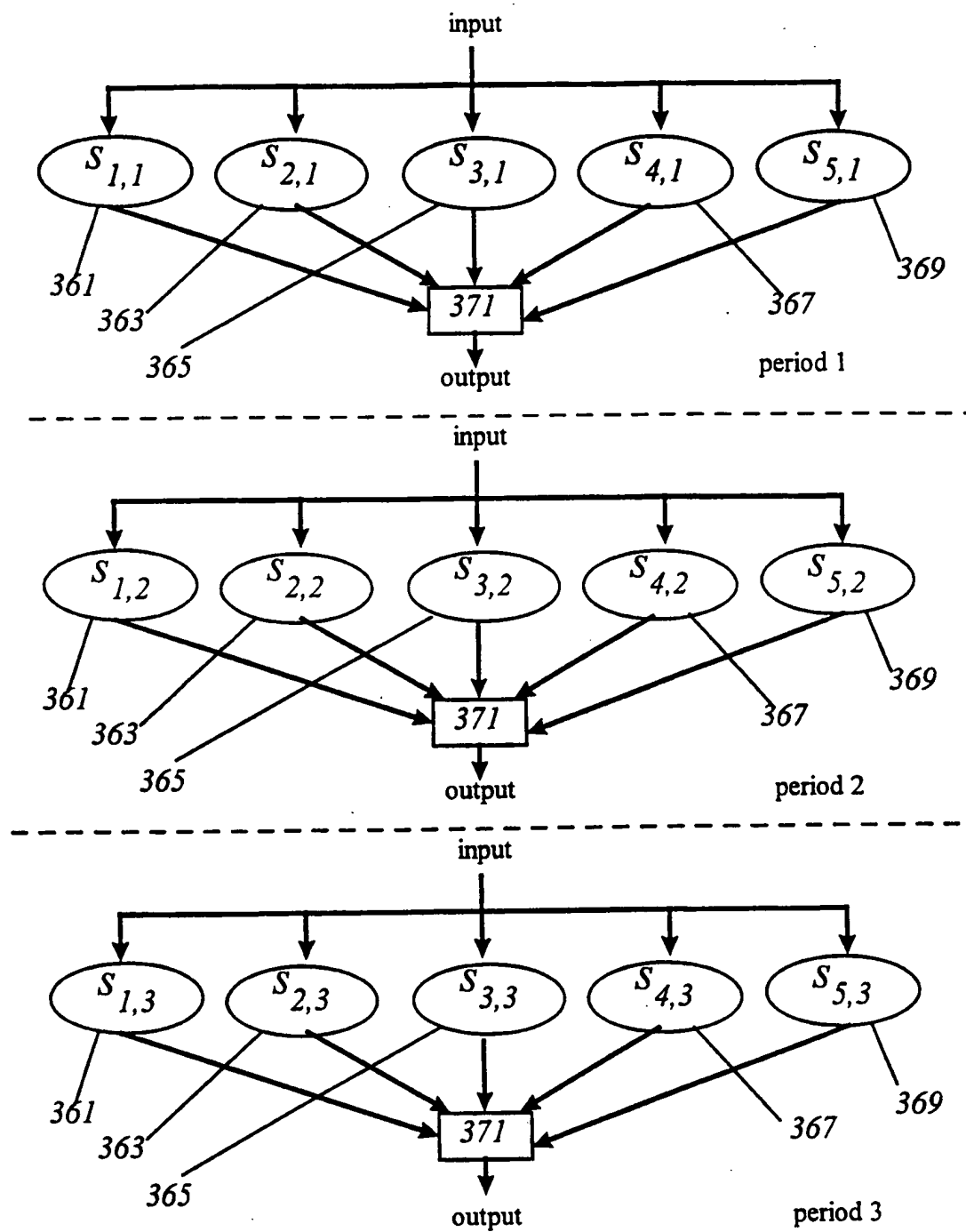


Figure 10

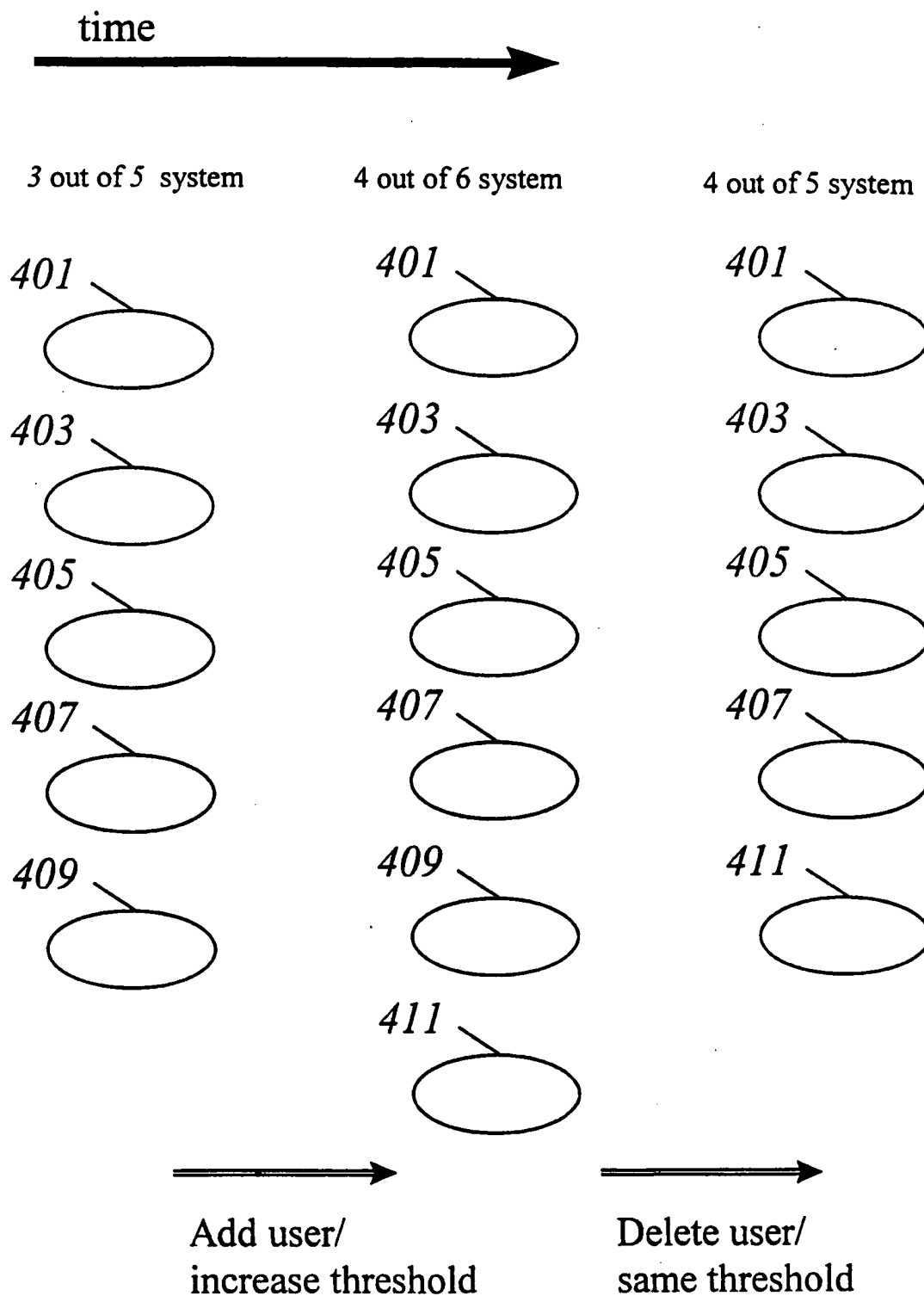


Figure 11

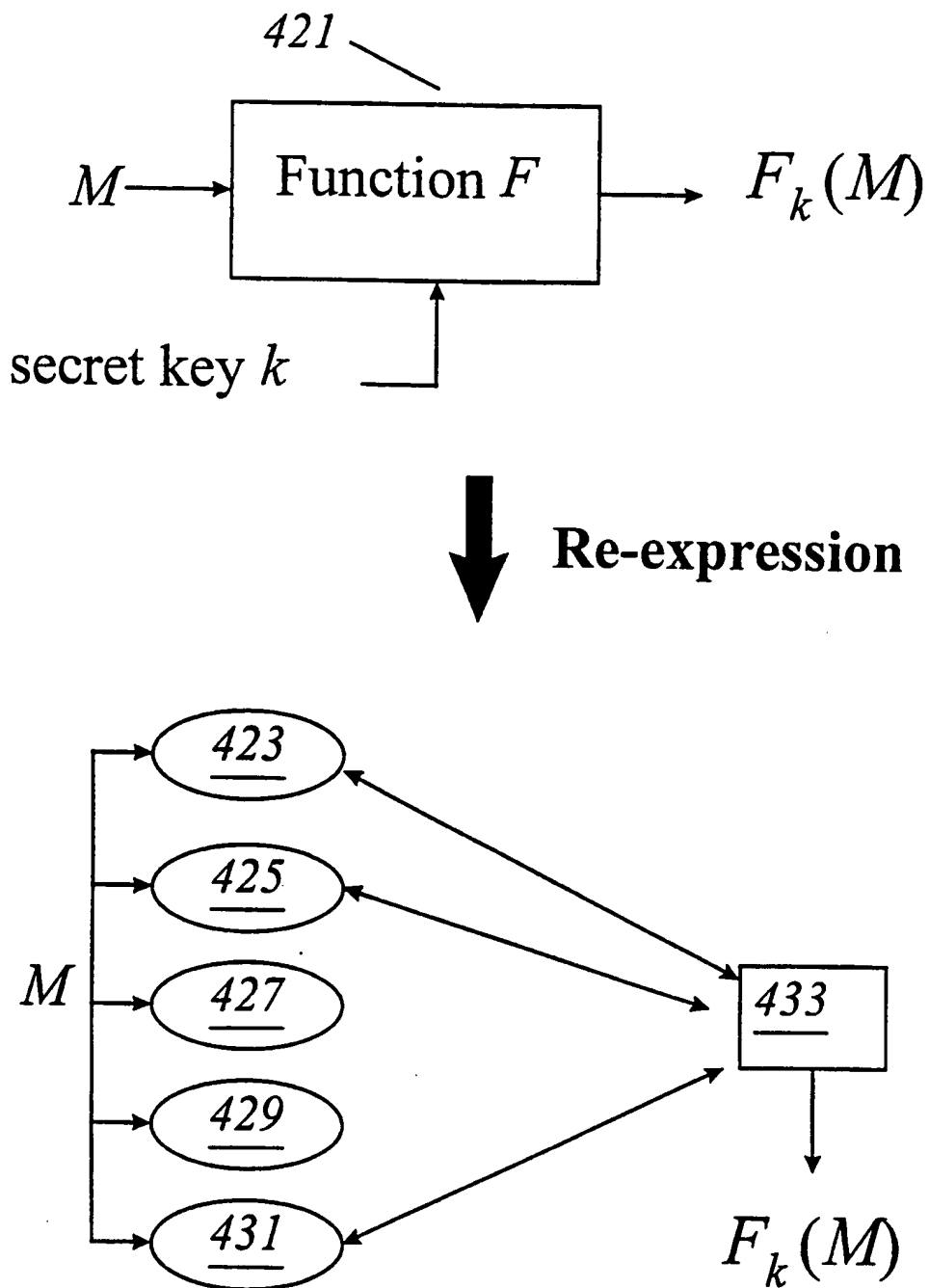


Figure 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/08299

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/30;

US CL :380/30,21,49

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/30,21,49,45

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS text search: Secret sharing

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|-----------|--|-----------------------|
| X | US 5,412,723 A (CANETTI et al.) 02 May 1995 (02.05.95) - see entire document. | 1 |
| X,P | US 5,625,692 A (HERZBERG et al.) 29 April 1997 (29.04.97) - see entire document | 1 |
| A | US 5,469,507 A (CANETTI et al.) 21 November 1995 (21.11.95) - see entire document. | 1 |
| A,P | US 5,708,714 A (LOPEZ et al.) 13 January 1998 (13.01.98)- see entire document. | 1 |
| A,E | US 5,764,767 A (BEIMEL et al.) 09 June 1998 (09.06.98) - see entire document. | 1 |

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

| | |
|---|--|
| * Special categories of cited documents: | *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention |
| *A* document defining the general state of the art which is not considered to be of particular relevance | *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone |
| *E* earlier document published on or after the international filing date | *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | *Z* document member of the same patent family |
| *O* document referring to an oral disclosure, use, exhibition or other means | |
| *P* document published prior to the international filing date but later than the priority date claimed | |

Date of the actual completion of the international search

17 JUNE 1998

Date of mailing of the international search report

27 JUL 1998

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

PINCHUS M. LAUFER *Diane Smith for*

Telephone No. (703) 306-4177